Embrace digital technology and move your business online to survive and thrive!

#GoDigitalWC Articles

Get tips and learn how to take your business online, click here

#GoDigitalWC Webinars

Hear from experts and thought leaders on digitizing your business, click here

#GoDigitalWC Tech Volunteers Initiative

Find out more about our FREE digital advisory support offer, click here

Article 16: An Introduction to the Protection of Personal Information Act (or POPI Act or POPIA)

Purpose of the Act

The increasing cases of theft and misuse of people's personal information has led to the need to promulgate regulations to protect personal information and one's right to privacy. The POPI Act sets out the minimum standards regarding accessing and 'processing' of any personal information belonging to another. The Act defines 'processing' as collecting, receiving, recording, organizing, retrieving, or the use, distribution or sharing of any such information.

The POPI Act (POPIA) was signed into law in November 2013 and the remaining provisions of the Act were due to come into effect on 1 April 2020, however given the current COVID-19 pandemic and emergency need to redeploy efforts, these were delayed. The President issued a Proclamation on 22 June 2020, commencing some sections of the POPI Act which came into effect on 1 July 2020, namely sections 2 to 38, 55 to 109, 111 and 114(1), (2) and (3). These sections largely deal with the application and exclusion provisions, the lawful processing of personal information and respective exemptions, the Information Officer, prior authorization, codes of conduct and provisions regulating direct marketing. Sections 110 and 114(4) are due to come into effect on 30 June 2021.

Defining personal information

Personal information is any information that may identify a person such as a name, surname, identity number, contact number, email address, religion, medical history, education, financial or any other information that is unique to an individual.

How this Act impacts you as a business owner

All organisations in South Africa (of any size) and individuals that are in a position to obtain, handle and store the personal information of another individual, whether it be in terms of their employment or as suppliers or service providers, must adhere to the requirements of the Act and implement steps to safeguard this information.

Companies have 12 months to get their systems and processes in place to comply with the Act, in this case 1 July 2021. Non-compliance could result in not only reputational damage and/or potential civil damages claims, but punitive fines up to R10 million or 10 years imprisonment, or a combination thereof.

Ensuring compliance to POPIA in your business

It is your responsibility as the business owner to ensure that all personal information is stored safely and not accessible to individuals that may misuse or share that information for any onerous intent. Here are a few practical steps you can put in place to safeguard personal information:

1. **Compile and document a strategy:** Formalize an IT security strategy by stipulating how the data is going to be protected (including data backup processes) and identify all the associated or potential risks such as data breaches, lost/stolen PCs/devices, staff leaving with databases etc. Consider how you would mitigate those risks, in other words have a response strategy in place. That way you will be better prepared should something go wrong. This strategy needs to be available, accessible and regularly monitored, reviewed and the safeguards re-addressed if need be.

2. **Protect against malware**: Secure all PCs, devices and your network through applying a firewall, ensuring passwords are confidential and complex, and that security software protection and antispam software for emails are in place. Enable automatic software updates and security settings on all devices. Ensure that any employees personal PCs/devices (used for business) and those being used for remote working are also secure. If you offer WiFi access, ensure that you use a strong encryption setting and turn off the SSID broadcasting function so as to make your network invisible. It is recommended that you read article 15 in this series ***Understanding Cyber Security***, to gain a greater understanding of how to protect your business against data breaches and cyber attacks.

3. **Use the cloud:** You may need to consider automating current paper record keeping and disposal systems. It is worth while looking into a reputable cloud service provider that can assist with storing information and implementing security measures. There are many to select from such as Microsoft, Amazon, IBM, Google, SAP, Salesforce, Oracle and many others including local companies with expertise in using these platforms.

4. **Inform employees:** It is critical that **everyone** in your business understands the company security policy and it's importance. Inform and train your staff on the POPIA compliant systems and processes, and ensure that they adhere to treating all information confidentially and with integrity. Regular refresher training is recommended and include this in the induction process for new employees at all levels.

5. **Gain consent from those concerned:** Ensure that you have the relevant authorization/consent from the respective individual or company to process and store their information, and that they understand what the information will be used for. Only collect the information relevant to the transaction with your business. It is always better to be upfront with your intentions around all data collected.

6. **Storage period:** Keep personal and confidential information only for as long as you need it. Determine the 'horizon' for when this data will no longer be needed, and when the time comes, destroy the data.

7. **Destroying records.** Carefully consider how best to erase, delete or destroy information when it is no longer justifiable to keep it. This in itself can present a risk so investigate what physical or digital 'shredding' and secure data deletion methods best work for your business.

It is important to note that you are obligated to inform an individual and the Information Regulator in cases where you or your staff believe that personal information has been compromised. The Act provides for limited exceptions where personal information can be shared in special circumstances, such as where it is required by law or instances for statistical purposes such as BEE or Employment Equity etc.

This is an ideal time to ensure your business embarks on the best practice record keeping and safety mechanisms to avoid non-compliance proactively.

You can also click on the following link https://www.seesa.co.za/wondering-how-to-comply-with-the-popi-act-start-here/ to find out more about practical measures to implement in your business.

The following recordings of POPI webinars also provide an additional source information and tips to incorporate the requirements into your business:

https://www.youtube.com/watch?v=XQhGh_T5Scs

https://www.youtube.com/watch?v=Qjpanc5Ial0

Who to contact for more information

You will find many online training and education programs on offer to assist you with fully understanding your role, rights and responsibilities in terms of the POPI Act. There are also many legal specialists that you could consult with to ensure you are on the right track.

Alternatively you can review the current POPI Act directly via : https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

Should you have any further questions or concerns please use the following link https://westerncapegov.custhelp.com/app/ask to get the answers you need.

References

https://www.comparethecloud.net/articles/10-practical-tips-for-keeping-your-business-data-secure/

https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

https://www.masthead.co.za/newsletter/the-protection-of-personal-information-act-popia-is-set-to-take-effect-on-1-july-2020/